REMARKS

Claims 1-12 are pending in the Application. The Abstract is objected to. Claim 1 is rejected under 35 U.S.C. §112, second paragraph. Claims 1-12 are rejected under 35 U.S.C. §103(a). Applicants respectfully traverse these rejections for at least the reasons stated below and respectfully request the Examiner to reconsider and withdraw these rejections.

Applicants note that claims 1, 5 and 9 were amended, as indicated above, not to overcome prior art but to more clearly claim the subject matter. Hence, no prosecution history estoppel arises from the amendments to claims 1, 5 and 9. *Festo Corp. v. Shoketsu Kinzoku Kogyo Kabushiki Co.*, 62 U.S.P.Q.2d 1705, 1711-12 (2002); 56 U.S.P.Q.2d 1865, 1870 (Fed. Cir. 2000). Further, the amendments made to claims 1, 5 and 9 were not made for a substantial reason related to patentability and therefore no prosecution history estoppel arises from such amendments. *See Festo Corp.*, 62 U.S.P.Q.2d 1705 at 1707 (2002); *Warner-Jenkinson Co. v. Hilton Davis Chemical Co.*, 41 U.S.P.Q.2d 1865, 1873 (1997).

I. OBJECTIONS TO THE SPECIFICATION:

The Examiner has objected to the Abstract for exceeding 150 words in length. Paper No. 3, page 2. Applicants amended the Abstract to have a length less than 150 words as indicated above. Applicants respectfully request the Examiner to withdraw the objection to the Abstract.

II. REJECTIONS UNDER 35 U.S.C. §112, SECOND PARAGRAPH:

The Examiner has rejected claim 1 under 35 U.S.C. §112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which Applicants regard as the invention. Paper No. 3, page 2. In particular, the Examiner states that in the limitation beginning with the word "encrypting" in claim 1 it is unclear whether the NA data is referring to the encrypted NA data. Paper No. 3, page 2. Applicants amended claims 1, 5 and 9 by including the term "encrypted" prior to the words "NA data" to clarify the meaning of this limitation.

Applicants respectfully assert that claim 1 is definite and distinctly claims the subject matter which Applicants regard as the invention. Accordingly, Applicants kindly request the Examiner to withdraw the rejection to claim 1 as being indefinite under 35 U.S.C. §112, second paragraph.

III. REJECTIONS UNDER 35 U.S.C. §103(a):

The Examiner has rejected claims 1-12 under 35 U.S.C. §103(a) as being unpatentable over Mirov et al. (U.S. Patent No. 6,138,236) (hereinafter "Mirov") in view of U.S. Patent No. 6,654,820 (hereinafter "Ishibashi") and in further view of Christeson et al. (U.S. Patent No. 5,579,522) (hereinafter "Christeson"). Applicants respectfully traverse these rejections for at least the reasons stated below and respectfully request the Examiner to reconsider and withdraw these rejections.

A. Mirov, Ishibashi and Christeson, taken singly or in combination, do not teach or suggest the following claim limitations.

Applicants respectfully assert that Mirov, Ishibashi and Christeson, taken singly or in combination, do not teach or suggest "encrypting normally unaccessible (NA) data with said symmetrical encryption key" as recited in claim 1 and similarly in claims 5 and 9. The Examiner cites column 4, lines 1-17 of Mirov as teaching the above-cited claim limitation. Paper No. 3, page 3. The Examiner further cited column 4, lines 42-55 as teaching storing encryption keys. Paper No. 3, page 3. In the passage of column 4, lines 42-55 of Mirov it taught storing a public key. Column 4, line 45. Hence, Applicants assuming that the Examiner asserts that the public key of Mirov teaches the encryption key in the recited claim. Applicants respectfully traverse the assertion that Mirov teaches the above-cited claim limitation.

Mirov instead teaches that during initialization of the computer system, the secure micro-code of the authentication section executes and directs the hash generator to generate a data hash of the unsecured micro-code programmed in the programmable section of the flash PROM. Column 4, lines 8-12. Mirov further teaches that the secure micro-code also directs the decryptor to calculate a verification hash. Column 4, lines 12-14. There is no language in the cited passage that teaches encrypting normally unaccessible data. Neither is there any language in the cited

passage that teaches encrypting normally unaccessible data using a symmetrical encryption key (Examiner asserts that the public key of Mirov teaches an encryption key). Therefore, the Examiner has not presented a *prima facie* case of obviousness in rejecting claims 1, 5 and 9, since the Examiner is relying upon an incorrect, factual predicate in support of the rejections. *In re Rouffet*, 47 U.S.P.Q.2d 1453, 1455 (Fed. Cir. 1998).

Applicants further assert that Mirov, Ishibashi and Christeson, taken singly or in combination, do not teach or suggest "storing said encrypted NA data and accessible non-encrypted (ANE) data in an unprotected electronically erasable programmable read only memory (EEPROM) with existing write protect algorithms" as recited in claim 1 and similarly in claims 5 and 9. The Examiner cites column 3, lines 55-65 of Mirov as teaching the above-cited claim limitation. Paper No. 3, page 3. Applicants respectfully traverse and assert that Mirov instead teaches a flash PROM which is divided into an authentication section and a programmable section. Column 3, lines 56-58. Mirov further teaches that the authentication section is a ROM. Column 3, lines 59-60. Mirov further teaches that the micro-code instructions contained in the authentication section are read-only. Column 3, lines 60-61. Mirov further teaches that the micro-code instructions contained in the programmable section are re-writable. Column 3, lines 61-63. Hence, Mirov teaches storing secured micro-code in the authentication section and teaches storing unsecured micro-code in the programmable section as illustrated in Figure 2. There is no language in the cited passage that teaches storing encrypted NA data in an unprotected EEPROM. As understood by the Applicants, the Examiner interprets secured micro-code in the authentication section as teaching encrypted NA data. However, there is no language in Mirov that teaches that the secured micro-code in the authentication section is encrypted. Therefore, the Examiner has not presented a *prima facie* case of obviousness in rejecting claims 1, 5 and 9, since the Examiner is relying upon an incorrect, factual predicate in support of the rejections. *In re Rouffet*, 47 U.S.P.Q.2d 1453, 1455 (Fed. Cir. 1998).

Claims 2-4, 6-8 and 10-12 each recite combinations of features including the above combinations, and thus are patentable over Mirov in view of Ishibashi and in

further view of Christeson for at least the above-stated reasons. Claims 2-4, 6-8 and 10-12 recite additional features, which, in combination with the features of the claims upon which they depend, are patentable over Mirov in view of Ishibashi and in further view of Christeson.

For example, Mirov, Ishibashi and Christeson, taken singly or in combination, do not teach or suggest "altering said ANE data by issuing an existing write request to said BIOS from said write protect algorithms for said EEPROM; and updating said ANE data in said EEPROM" as recited in claim 2 and similarly in claims 6 and 10. The Examiner cites column 3, lines 55-65 of Mirov as teaching the above-cited claim limitation. Paper No. 3, page 4. Applicants respectfully traverse and assert that Mirov instead teaches that Mirov instead teaches a flash PROM which is divided into an authentication section and a programmable section. Column 3, lines 56-58. Mirov further teaches that the authentication section is a ROM. Column 3, lines 59-60. Mirov further teaches that the micro-code instructions contained in the authentication section are read-only. Column 3, lines 60-61. Mirov further teaches that the micro-code instructions contained in the programmable section are re-writable. Column 3, lines 61-63. Hence, Mirov teaches storing secured micro-code in the authentication section and teaches storing unsecured micro-code in the programmable section as illustrated in Figure 2. There is no language in the cited passage that teaches altering ANE data. Neither is there any language in the cited passage that teaches altering ANE data by issuing an existing write request. Neither is there any language in the cited passage that teaches altering ANE data by issuing an existing write request to the BIOS. Neither is there any language in the cited passage that teaches altering ANE data by issuing an existing write request to the BIOS from the write protect algorithms for the EEPROM. Neither is there any language in the cited passage that teaches updating ANE data. Neither is there any language in the cited passage that teaches updating ANE data in the EEPROM. Therefore, the Examiner has not presented a *prima facie* case of obviousness in rejecting claims 2, 6 and 10, since the Examiner is relying upon an incorrect, factual predicate in support of the rejections. *In re Rouffet*, 47 U.S.P.Q.2d 1453, 1455 (Fed. Cir. 1998).

Applicants further assert that Mirov, Ishibashi and Christeson, taken singly or in combination, do not teach or suggest "accessing said NA data via a change request issued to said BIOS over a secure communication link; validating said change request; retrieving said symmetrical encryption key by said BIOS in response to said validated change request; using said symmetrical encryption key to decrypt and alter said NA data; encrypting said altered NA data using said symmetrical encryption key; and storing said altered encrypted NA data in said EEPROM" as recited in claim 3 and similarly in claims 7 and 11. The Examiner cites column 10, line 54 – column 12, line 67 and Figures 5 and 6 of Christeson as teaching the above-cited claim limitations. Paper No. 3, page 4. Applicants respectfully traverse.

Christeson instead teaches the dynamic BIOS update processing logic. Column 10, line 54 – column 12, line 67. There is no language in the cited passage that teaches accessing NA data. Neither is there any language in the cited passage that teaches accessing NA data via a change request issued to the BIOS. Neither is there any language in the cited passage that teaches accessing NA data via a change request issued to the BIOS over a secure communication link. Neither is there any language in the cited passage that teaches validating the change request. Neither is there any language in the cited passage that teaches retrieving a symmetrical encryption key. Neither is there any language in the cited passage that teaches retrieving a symmetrical encryption key by the BIOS. Neither is there any language in the cited passage that teaches retrieving a symmetrical encryption key by the BIOS in response to the validated change request. Neither is there any language in the cited passage that teaches using a symmetrical encryption key to decrypt. Neither is there any language in the cited passage that teaches using a symmetrical encryption key to decrypt and alter the NA data. Neither is there any language in the cited passage that teaches encrypting the altered NA data. Neither is there any language in the cited passage that teaches encrypting the altered NA data using the symmetrical encryption key. Neither is there any language in the cited passage that teaches storing altered encrypted NA data. Neither is there any language in the cited passage that teaches storing altered encrypted NA data in the EEPROM. Therefore, the Examiner has not presented a *prima facie* case of obviousness in rejecting claims 3, 7 and 11, since the

Examiner is relying upon an incorrect, factual predicate in support of the rejections. *In re Rouffet*, 47 U.S.P.Q.2d 1453, 1455 (Fed. Cir. 1998).

Applicants further assert that Mirov, Ishibashi and Christeson, taken singly or in combination, do not teach or suggest "hashing said ANE data and encrypting said Hash with said symmetrical encryption key; storing said encrypted Hash with said ANE data; computing a Hash of configuration data in said ANE data on a boot-up request; decrypting said stored encrypted Hash of said configuration data; comparing said decrypted Hash of said stored configuration data to said computed Hash of said configuration data from said ANE data; booting normally in response to a compare of said decrypted Hash and said computed hash; and issuing tamper notification and initiating recovery processes on a non-compare of said decrypted Hash and said computed hash" as recited in claim 4 and similarly in claims 8 and 12. The Examiner cites column 2, lines 21-32 and column 3, line 55 – column 5, line 50 of Mirov as teaching the above-cited claim limitation. Paper No. 3, page 5. Applicants respectfully traverse.

Mirov instead teaches a computer system where a portion of code/data stored in a non-volatile memory device can be dynamically modified or updated without removing any covers or parts from the computer system. Column 2, lines 17-20. Mirov further teaches that the computer system of the preferred embodiment includes a flash memory component coupled to the bus for storing non-volatile code and data. Column 2, lines 33-34. Mirov further teaches that using the present invention, the contents of the flash memory may be replaced, modified, updated or reprogrammed without the need for removing and/or replacing any computer system hardware components. Column 2, lines 36-40. There is no language in the cited passages that teaches hashing ANE data. Neither is there any language in the cited passages that teaches hashing ANE data and encrypting the Hash with a symmetrical encryption key. Neither is there any language in the cited passages that teaches storing an encrypted Hash. Neither is there any language in the cited passages that teaches storing an encrypted Hash with the ANE data. Neither is there any language in the cited passages that teaches computing a Hash of configuration data. Neither is there any language in the cited passages that teaches computing a Hash of configuration

data in the ANE data. Neither is there any language in the cited passages that teaches computing a Hash of configuration data in the ANE data on a boot-up request. Neither is there any language in the cited passages that teaches decrypting the stored encrypted Hash of the configuration data. Neither is there any language in the cited passages that teaches comparing the decrypted Hash of the stored configuration data to the computed Hash of the configuration data from the ANE data. Neither is there any language in the cited passages that teaches booting normally in response to a compare of the decrypted Hash and the computed hash. Neither is there any language in the cited passages that teaches issuing tamper notification. Neither is there any language in the cited passages that teaches issuing tamper notification and initiating recovery processes. Neither is there any language in the cited passages that teaches issuing tamper notification and initiating recovery processes on a non-compare of the decrypted Hash and the computed hash. Therefore, the Examiner has not presented a *prima facie* case of obviousness in rejecting claims 4, 8 and 12, since the Examiner is relying upon an incorrect, factual predicate in support of the rejections. *In re Rouffet*, 47 U.S.P.Q.2d 1453, 1455 (Fed. Cir. 1998).

B. Examiner has not provided a source of motivation or objective evidence for modifying Mirov to provide a protected storage accessible only by BIOS, as recited in claims 1, 5 and 9.

Most if not all inventions arise from a combination of old elements. *See In re Rouffet*, 47 U.S.P.Q.2d 1453, 1457 (Fed. Cir. 1998). Obviousness is determined from the vantage point of a hypothetical person having ordinary skill in the art to which the patent pertains. *In re Rouffet*, 47 U.S.P.Q.2d 1453, 1457 (Fed. Cir. 1998). Therefore, an Examiner may often find every element of a claimed invention may often be found in the prior art. *Id.* However, identification in the prior art of each individual part claimed is insufficient to defeat patentability of the whole claimed invention. *See Id.* In order to establish a *prima facie* case of obviousness, the Examiner must show reasons that the skilled artisan, confronted with the same problems as the inventor and with no knowledge of the claimed invention, would select the elements from the cited prior art references for combination in the manner claimed. *In re Rouffet*, 47 U.S.P.Q.2d 1453, 1458 (Fed. Cir. 1998). That is, the

Examiner must provide some suggestion or motivation, either in the references themselves, the knowledge of one of ordinary skill in the art, or, in some case, the nature of the problem to be solved, to modify the reference or to combine reference teachings. *See In re Dembiczak*, 175 F.3d 994, 999, 50 U.S.P.Q.2d 1614, 1617 (Fed. Cir. 1999). Whether the Examiner relies on an express or an implicit showing, the Examiner must provide particular findings related thereto. *In re Kotzab*, 55 U.S.P.Q.2d 1313, 1317 (Fed. Cir. 2000).

The Examiner admits that Mirov does not teach providing a protected storage accessible only by BIOS, as recited in claim 1 and similarly in claims 5 and 9. The Examiner modifies Mirov with Ishibashi to include the above-cited claim limitation "for secure protection of the key from being tampered by computer users." Paper No. 3, page 3. The Examiner's motivation is insufficient to establish a *prima facie* case of obviousness in rejecting claims 1-12.

The Examiner has not provided a source for his motivation for modifying Mirov to include the above-cited claim limitation. The Examiner simply states "for secure protection of the key from being tampered by computer users" as motivation for modifying Mirov to include the above-cited claim limitation. The motivation to modify Mirov must come from one of three possible sources: the nature of the problem to be solved, the teachings of the prior art, and the knowledge of persons of ordinary skill in the art. *In re Rouffet*, 149 F.3d 1350, 1357, 47 U.S.P.Q.2d 1453, 1457-48 (Fed. Cir. 1998). The Examiner has not provided any evidence that his motivation comes from any of these sources. Instead, the Examiner is relying upon his own subjective opinion which is insufficient to support a *prima facie* case of obviousness. *In re Lee*, 61 U.S.P.Q.2d 1430, 1434 (Fed. Cir. 2002). Consequently, the Examiner's motivation is insufficient to support a *prima facie* case of obviousness for rejecting claims 1-12. *Id.*

Furthermore, the Examiner's motivation ("for secure protection of the key from being tampered by computer users") does not provide reasons that the skilled artisan, confronted with the same problems as the inventor and with no knowledge of

the claimed invention, would modify Mirov to include the above-cited missing claim limitation from claims 1, 5 and 9. According, the Examiner has not presented a *prima facie* case of obviousness for rejecting claims 1-12. *In re Rouffet*, 47 U.S.P.Q.2d 1453, 1458 (Fed. Cir. 1998).

Mirov addresses the problem of providing an apparatus for authenticating firmware programmed in a boot PROM and methods that enable programming access to the boot PROM without compromising the authenticity of the firmware that overcomes the disadvantages of disassembling the computer system. Column 1, line 65 – column 2, line 3. The Examiner has not provided any reasons as to why one skilled in the art would modify Mirov, which teaches enabling programming access to the boot PROM without compromising the authenticity of the firmware that overcomes the disadvantages of disassembling the computer system, to provide protected storage accessible only by BIOS (Examiner admits that Mirov does not teach this limitation). The Examiner's motivation ("for secure protection of the key from being tampered by computer users") does not provide such reasoning. That is, the Examiner's motivation does not provide reasons as to why one skilled in the art would modify a reference, whose purpose is to enable programming access to the boot PROM without compromising the authenticity of the firmware, to provide protected storage accessible only by BIOS. The Examiner must provide objective evidence in modifying Mirov to include the above-cited missing limitation of claims 1, 5 and 9. *In re Lee*, 61 U.S.P.Q.2d 1430, 1434 (Fed. Cir. 2002). Instead, the Examiner is merely relying upon his own subjective opinion which is insufficient to support a *prima facie* case of obviousness in rejecting claims 1-12. *Id.* Consequently, the Examiner's motivation is insufficient to support a *prima facie* case of obviousness for rejecting claims 1-12. *Id.*

Further, the Examiner's conclusion of obviousness is based on improper hindsight reasoning. The Examiner is relying solely on knowledge gleaned from the Applicants' disclosure which is impermissible. *In re McLaughlin*, 443 F.2d 1392, 1395, 170 U.S.P.Q. 209, 212 (C.C.P.A. 1971). The Examiner appears to be using knowledge from the Specification as support for his motivation. Applicants

respectfully direct the Examiner's attention to at least page 6, lines 10-11, 19-23 and page 7, lines 3-7 of the Specification which discusses using a protected storage for the symmetrical encryption key which provides secure protection. The Examiner must submit objective evidence, that is not gleaned from the Applicants' disclosure, in support of modifying Mirov with Ishibashi to provide protected storage accessible only by BIOS in order to support a *prima facie* case of obviousness for rejecting claims 1-12. *In re Lee*, 61 U.S.P.Q.2d 1430, 1434 (Fed. Cir. 2002). Consequently, the Examiner's motivation is insufficient to support a *prima facie* case of obviousness for rejecting claims 1-12. *Id.*; M.P.E.P. §2145.

C. The Examiner has not provided a motivation for modifying Mirov to store a symmetrical encryption key in a protected storage, as recited in claim 1 and similarly in claims 5 and 9.

The Examiner admits that Mirov does not teach storing a symmetrical encryption key. Paper No. 3, page 3. Further, the Examiner admits that Mirov does not teach a protected storage. Paper No. 3, page 3. The Examiner asserts that a symmetrical encryption key is well known. Paper No. 3, page 3. While a symmetrical encryption key may be well known, Applicants respectfully traverse the assertion that storing a symmetrical encryption key is well known. Applicants respectfully request the Examiner to provide a reference that teaches storing a symmetrical encryption key pursuant to M.P.E.P. §2144.03.

Further, the Examiner asserts that column 6, lines 22-31 of Ishibashi teaches a protected storage which is accessibly only by BIOS code. The Examiner then modifies Mirov with Ishibashi to thereby teach storing a symmetrical encryption key in a protected storage, which is accessible only by BIOS code. Paper No. 3, page 3. However, the Examiner has not provided any motivation for modifying Mirov with Ishibashi to include the above-cited claim limitation. In order to establish a *prima facie* case of obviousness, the Examiner must provide some suggestion or motivation, either in the references themselves, the knowledge of one of ordinary skill in the art, or, in some case, the nature of the problem to be solved, to modify Angelo with Sowa to include the above-cited claim limitation. *See In re Dembiczak*, 175 F.3d 994, 999,

50 U.S.P.Q.2d 1614, 1617 (Fed. Cir. 1999); M.P.E.P. §2143. Since the Examiner has not provided such motivation, the Examiner has not presented a *prima facie* case of obviousness in rejecting claims 1-12. M.P.E.P. §2143.

D. The Examiner has not provided a source of motivation or objective evidence for modifying Mirov to store a symmetrical encryption key as well as to encrypt normally unaccessible (NA) data with the symmetrical encryption key, as recited in claims 1, 5 and 9.

As stated above, the Examiner must provide some suggestion or motivation, either in the references themselves, the knowledge of one of ordinary skill in the art, or, in some case, the nature of the problem to be solved, to modify the reference or to combine reference teachings. *See In re Dembiczak*, 175 F.3d 994, 999, 50 U.S.P.Q.2d 1614, 1617 (Fed. Cir. 1999). Whether the Examiner relies on an express or an implicit showing, the Examiner must provide particular findings related thereto. *In re Kotzab*, 55 U.S.P.Q.2d 1313, 1317 (Fed. Cir. 2000).

The Examiner admits that Mirov does not teach storing a symmetrical encryption key, as recited in claim 1 and similarly in claims 5 and 9. Further, the Examiner admits that Mirov does not teach encrypting normally accessible (NA) data with the symmetrical encryption key, as recited in claim 1 and similarly in claims 5 and 9. The Examiner modifies Mirov to include the above-cited claim limitations "for its speed." Paper No. 3, page 3. The Examiner's motivation is insufficient to establish a *prima facie* case of obviousness in rejecting claims 1-12.

The Examiner has not provided a source for his motivation for modifying Mirov to include the above-cited claim limitations. The Examiner simply states "for its speed" as motivation for modifying Mirov to include the above-cited claim limitations. The motivation to modify Mirov must come from one of three possible sources: the nature of the problem to be solved, the teachings of the prior art, and the knowledge of persons of ordinary skill in the art. *In re Rouffet*, 149 F.3d 1350, 1357, 47 U.S.P.Q.2d 1453, 1457-48 (Fed. Cir. 1998). The Examiner has not provided any evidence that his motivation comes from any of these sources. Instead, the Examiner is relying upon his own subjective opinion which is insufficient to support a *prima*

facie case of obviousness. *In re Lee*, 61 U.S.P.Q.2d 1430, 1434 (Fed. Cir. 2002). Consequently, the Examiner's motivation is insufficient to support a *prima facie* case of obviousness for rejecting claims 1-12. *Id.*

Furthermore, the Examiner's motivation ("for its speed") does not provide reasons that the skilled artisan, confronted with the same problems as the inventor and with no knowledge of the claimed invention, would modify Mirov to include the above-cited missing claim limitations from claims 1, 5 and 9. According, the Examiner has not presented a *prima facie* case of obviousness for rejecting claims 1-12. *In re Rouffet*, 47 U.S.P.Q.2d 1453, 1458 (Fed. Cir. 1998).

Mirov addresses the problem of providing an apparatus for authenticating firmware programmed in a boot PROM and methods that enable programming access to the boot PROM without compromising the authenticity of the firmware that overcomes the disadvantages of disassembling the computer system. Column 1, line 65 – column 2, line 3. The Examiner has not provided any reasons as to why one skilled in the art would modify Mirov, which teaches enabling programming access to the boot PROM without compromising the authenticity of the firmware that overcomes the disadvantages of disassembling the computer system, to store a symmetrical encryption key (Examiner admits that Mirov does not teach this limitation) or to encrypt normally unaccessible (NA) data with the symmetrical encryption key (Examiner admits that Mirov does not teach this limitation). The Examiner's motivation ("for its speed") does not provide such reasoning. The Examiner has not provided a rationale connection between "speed" and the limitation of storing a symmetrical encryption key, as recited in claims 1, 5 and 9. Neither has the Examiner provide a rationale connection between "speed" and the limitation of encrypting normally unaccessible (NA) data with the symmetrical encryption key, as recited in claims 1, 5 and 9. The Examiner must provide objective evidence in modifying Mirov to include the above-cited missing limitations of claims 1, 5 and 9. *In re Lee*, 61 U.S.P.Q.2d 1430, 1434 (Fed. Cir. 2002). Instead, the Examiner is merely relying upon his own subjective opinion which is insufficient to support a *prima facie* case of obviousness in rejecting claims 1-12. *Id.* Consequently, the

Examiner's motivation is insufficient to support a *prima facie* case of obviousness for rejecting claims 1-12. *Id.*

E. By modifying Mirov to have a symmetrical encryption key, the principle of operation of Mirov would change.

If the proposed modification or combination of the prior art would change the principle of operation of the prior art invention being modified, then the teachings of the references are not sufficient to render the claims *prima facie* obvious. *In re Ratti*, 370 F.2d 810, 123 U.S.P.Q. 349 (C.C.P.A. 1959). Further, if the proposed modification would render the prior art invention being modified unsatisfactory for its intended purpose, then there is no suggestion or motivation to make the proposed modification. *In re Gordon*, 733 F.2d 900, 221 U.S.P.Q. 1125 (Fed. Cir. 1984). For the reasons discussed below, Appellants submit that by modifying Mirov to include a symmetrical encryption key as suggested by the Examiner, the principle of operation in Mirov would change and subsequently render the operation of Mirov to perform its purpose unsatisfactorily.

Mirov teaches a flash PROM (18) having an authentication section (45) and a programmable section (55) that affords ease in updating the flash PROM (18) with new micro-code without compromising security. Column 5, lines 16-19. Mirov further teaches that by implementing public-key cryptography having a private key and a public key to verify the programmable section (55) with the authentication section (45) assures that the programmable section of the micro-code is proper and authentic. Column 5, lines 19-23. Mirov further teaches that the integrity of the unsecured micro-code (58) of the programmable section (55) is also verified when the verification hash matches the data hash. Column 5, lines 23-25. Mirov further teaches that the private key is used for the generation of the verification hash. Column 4, lines 59-60. Mirov further teaches that the purpose of Mirov is to provide an apparatus for authenticating firmware programmed in a boot PROM and enable programming access to the boot PROM without compromising the authenticity of the firmware. Column 1, line 65 – column 2, line 3.

The Examiner admits that Mirov does not teach a symmetrical encryption key. Paper No. 3, page 3. The Examiner proposes modifying Mirov to include a symmetrical encryption key. Paper No. 3, page 3. However, by modifying Mirov to include a symmetrical encryption key, then Mirov would no longer be implementing an asymmetric cryptography system (the use of a private key and a public key) but instead implementing a symmetric cryptography system (the use of a single symmetric encryption key).

By implementing a symmetric cryptography system, Mirov would be forced to use a single secret key to verify the programmable section of the micro-code is proper and authentic. Further, Mirov would be forced to use a single secret key to verify the integrity of the unsecured micro-code (58) of the programmable section (55) when the verification hash (now be generated by the single secret key) matches the data hash. The use of a single key to perform these functions is not as secure as using a public/private key pair. Using a single key to encrypt and decrypt is not as secure since there is a problem with providing the key to the recipient (referring to the lack of security with using a single key). See definition of cryptography at www.techweb.com/encyclopedia. In asymmetric cryptography, the public key is published for everyone; however, the private key is kept secret and is never in transit and remains invulnerable. See definition of cryptography at www.techweb.com/encyclopedia. Hence, by modifying Mirov to include a symmetrical encryption key and use a symmetric cryptography system, Mirov may no longer be able to enable programming access to the boot PROM without compromising the authenticity of the firmware (stated purpose of Mirov). Thus, by modifying Mirov to include a symmetrical encryption key, the principle of operation in Mirov would change, and subsequently render the operation of Mirov to perform its purpose unsatisfactorily. Therefore, the Examiner has not presented a *prima facie* case of obviousness for rejecting claims 1-12. *In re Ratti*, 270 F.2d 810, 123 U.S.P.Q. 349 (C.C.P.A. 1959); *In re Gordon*, 733 F.2d 900, 221 U.S.P.Q. 1125 (Fed. Cir. 1984).

F. Applicants confused over the citing of Christeson with respect to claims 1, 5 and 9.

The Examiner states that Mirov does not teach remotely altering data but that Christeson does at column 2, lines 16-19. Paper No. 3, pages 3-4. The Examiner then provides motivation for modifying Mirov with Christeson to remotely alter data. Paper No. 3, page 4. However, there is no specific limitation of "remotely altering data" as asserted by the Examiner in claim 1 or similarly in claims 5 and 9. Applicants respectfully request the Examiner to particularly identify the reasons for citing Christeson pursuant to 37 C.F.R. §1.104(c)(2), i.e., identify which limitation in claim 1 that Mirov does not teach and that Christeson allegedly teaches.

G. The Examiner has not provided a motivation for modifying Mirov with Christeson to include the limitations of claims 3, 7 and 11.

The Examiner admits that Mirov does not teach the limitations of claim 3 and similarly in claims 7 and 11. Paper No. 3, page 4. The Examiner asserts that Christeson teaches the limitations of claim 3 and similarly in claims 7 and 11. Paper No. 3, page 4. The Examiner then modifies Mirov with Christeson to incorporate the limitations of claims 3, 7 and 11. Paper No. 3, page 4. However, the Examiner has not provided any motivation for modifying Mirov with Christeson to include the claim limitations of claims 3, 7 and 11. In order to establish a *prima facie* case of obviousness, the Examiner must provide some suggestion or motivation, either in the references themselves, the knowledge of one of ordinary skill in the art, or, in some case, the nature of the problem to be solved, to modify Mirov with Christeson to include the claim limitations of claims 3, 7 and 11. *See In re Dembiczak*, 175 F.3d 994, 999, 50 U.S.P.Q.2d 1614, 1617 (Fed. Cir. 1999); M.P.E.P. §2143. Since the Examiner has not provided such motivation, the Examiner has not presented a *prima facie* case of obviousness in rejecting claims 3, 7 and 11. M.P.E.P. §2143.

IV. CONCLUSION

As a result of the foregoing, it is asserted by Applicants that claims 1-12 in the Application are in condition for allowance, and Applicants respectfully request an allowance of such claims. Applicants respectfully request that the Examiner call Applicants' attorney at the below listed number if the Examiner believes that such a discussion would be helpful in resolving any remaining issues.

Respectfully submitted,

WINSTEAD SECHREST & MINICK P.C.

Attorneys for Applicants

By: _____

Robert A. Voigt, Jr.
Reg. No. 47,159
Kelly K. Kordzik
Reg. No. 36,571

P.O. Box 50784
Dallas, TX 75201
(512) 370-2832

Austin_1 298602v.1